

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-89668

(P2000-89668A)

(43) 公開日 平成12年3月31日 (2000.3.31)

(51) Int.Cl.<sup>7</sup>

G 0 9 C 1/00

識別記号

6 2 0

F I

G 0 9 C 1/00

テーマコード(参考)

6 2 0 Z

審査請求 未請求 請求項の数12 O L (全 10 頁)

(21) 出願番号

特願平10-262036

(22) 出願日

平成10年9月16日 (1998.9.16)

(71) 出願人 000006297

村田機械株式会社

京都府京都市南区吉祥院南落合町3番地

(71) 出願人 597008636

笠原 正雄

大阪府箕面市栗生外院4丁目15番3号

(72) 発明者 笠原 正雄

大阪府箕面市栗生外院4丁目15番3号

(72) 発明者 村上 恭通

京都府京都市伏見区竹田向代町136番地

村田機械株式会社本社工場内

(74) 代理人 100078868

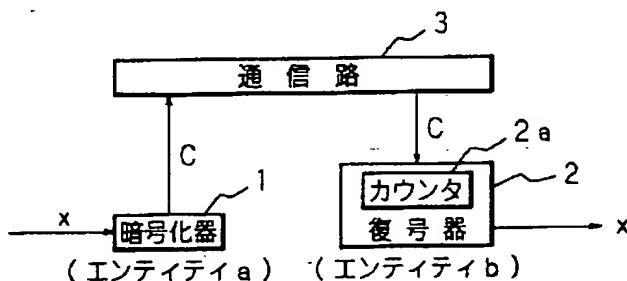
弁理士 河野 登夫

(54) 【発明の名称】 暗号化方法、復号方法、暗号化・復号方法及び暗号通信システム

(57) 【要約】

【課題】 高速の復号が可能な積和型暗号の暗号化・復号方法を提供する。

【解決手段】 平文ベクトル  $m = (m_0, m_1, \dots, m_{K-1})$  と基数ベクトル  $B = (B_0, B_1, \dots, B_{K-1})$  とを用いた内積により暗号文  $C = m_0 B_0 + m_1 B_1 + \dots + m_{K-1} B_{K-1}$  を得る積和型の暗号方式であつて、 $B_i$  ( $0 \leq i \leq K-1$ ) を  $B_i = b_0 b_1 \dots b_i$  に設定する。



## 【特許請求の範囲】

【請求項1】 平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて暗号文 $C = m_0 B_0 + m_1 B_1 + \dots + m_{K-1} B_{K-1}$ を得る暗号化方法において、前記 $B_i$  ( $0 \leq i \leq K-1$ )を整数 $b_i$ を用いて $B_i = b_0 b_1 \dots b_i$ に設定することを特徴とする暗号化方法。

【請求項2】 前記Kは2のべき乗数である請求項1記載の暗号化方法。

【請求項3】 請求項1によって暗号化された前記暗号文Cを復号する復号方法であって、以下のアルゴリズムにより暗号文Cから平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めることを特徴とする復号方法。

ステップ0

$$C_0 = C / b_0$$

$$m_0 \equiv C_0 \pmod{b_1}$$

ステップi ( $i = 1 \sim K-2$ )

$$C_i = (C_{i-1} - m_{i-1}) / b_i$$

$$m_i \equiv C_i \pmod{b_{i+1}}$$

ステップK-1

$$m_{K-1} = (C_{K-2} - m_{K-2}) / b_{K-1}$$

【請求項4】 平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて暗号文 $C = m_0 B_0 + m_1 B_1 + \dots + m_{K-1} B_{K-1}$ を得る暗号化方法において、

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (b)$$

暗号文Cに対して、中間復号文Mを式(c)のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod{P} \quad \dots (c)$$

この中間復号文Mを以下のアルゴリズムにより復号して平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めるステップと

ステップ0

$$M_0 = M / b_0$$

$$m_0 \equiv M_0 \pmod{b_1}$$

ステップi ( $i = 1 \sim K-2$ )

$$M_i = (M_{i-1} - m_{i-1}) / b_i$$

$$m_i \equiv M_i \pmod{b_{i+1}}$$

ステップK-1

$$m_{K-1} = (M_{K-2} - m_{K-2}) / b_{K-1}$$

暗号文Cに対して、中間復号文Mを式(f)のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod{P} \quad \dots (f)$$

この中間復号文Mを以下のアルゴリズムにより復号して平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めるステップと

【2分割アルゴリズム】

第1ステップ

$$ML \equiv M \pmod{B_{K/2}}$$

\*  $B_1 + \dots + m_{K-1} B_{K-1}$ を得る暗号化方法において、前記 $B_i$  ( $0 \leq i \leq K-1$ )を整数 $b_i$ 、乱数 $v_i$ を用いて $B_i = v_i b_0 b_1 \dots b_i$ に設定することを特徴とする暗号化方法。

【請求項5】 乱数ベクトル $v = (v_0, v_1, \dots, v_{K-1})$ を用いて暗号文 $C = m_0 v_0 B_0 + m_1 v_1 B_1 + \dots + m_{K-1} v_{K-1} B_{K-1}$ を得る請求項1記載の暗号化方法。

【請求項6】 前記K個の $b_i$ の集合を複数組準備し、それぞれの集合毎に暗号文を得るようにした請求項1または4記載の暗号化方法。

【請求項7】 平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて前記平文を暗号文に変換し、その暗号文を元の平文に変換する暗号化・復号方法において、

前記 $B_i$  ( $0 \leq i \leq K-1$ )を整数 $b_i$ を用いて $B_i = b_0 b_1 \dots b_i$ に設定するステップと、

$w < P$  ( $P$ :素数)を満たす $w$ を選択し、式(a)により公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求めるステップと、

$$c_i \equiv w B_i \pmod{P} \quad \dots (a)$$

平文ベクトル $m$ と公開鍵ベクトル $c$ との内積により、式(b)に示す暗号文Cを作成するステップと、

※を有することを特徴とする暗号化・復号方法。

【請求項8】 平文をK ( $K$ は2のべき乗数)分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

前記 $B_i$  ( $0 \leq i \leq K-1$ )を整数 $b_i$ を用いて $B_i = b_0 b_1 \dots b_i$ に設定するステップと、

$w < P$  ( $P$ :素数)を満たす $w$ を選択し、式(d)により公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求めるステップと、

$$c_i \equiv w B_i \pmod{P} \quad \dots (d)$$

平文ベクトル $m$ と公開鍵ベクトル $c$ との内積により、式(e)に示す暗号文Cを作成するステップと、

※40 (e)に示す暗号文Cを作成するステップと、

第2ステップ

$$MR = (M - ML) / B_{K/2}$$

【高速アルゴリズム】  $ML$ 、 $MR$ に対して再び2分割アルゴリズムを適用する。4分割された中間復号文のそれぞれに再び2分割アルゴリズムを適用する。このようなことを繰り返すを有することを特徴とする暗号化・復号方法。

【請求項9】 平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて暗号文Cを作成するステップと、

$1, \dots, B_{K-1}$ ) とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、前記  $B_i$  ( $0 \leq i \leq K-1$ ) を式 (g) にて設定するステップと、

$$B_i = v_i b_0 b_1 \dots b_i \quad \dots (g)$$

但し、 $v_i$  : 乱数

$b_i$  : 整数

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (i)$$

暗号文  $C$  に対して、中間復号文  $M$  を式 (j) のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod{P} \quad \dots (j)$$

この中間復号文  $M$  を以下のアルゴリズムにより復号して平文ベクトル  $m = (m_0, m_1, \dots, m_{K-1})$  を求めるステップと

ステップ 0

$$M_0 = C / b_0$$

$$m_0 \equiv M_0 v_0^{-1} \pmod{b_1}$$

ステップ  $i$  ( $i = 1 \sim K-2$ )

$$M_i = (M_{i-1} - m_{i-1} v_{i-1}) / b_i$$

$$m_i \equiv M_i v_i^{-1} \pmod{b_{i+1}}$$

ステップ  $K-1$

$$M_{K-1} = (M_{K-2} - m_{K-2} v_{K-2}) / b_{K-1}$$

$$m_{K-1} = M_{K-1} / v_{K-1}$$

を有することを特徴とする暗号化・復号方法。

【請求項 10】 平文を  $K$  分割した平文ベクトル  $m = (m_0, m_1, \dots, m_{K-1})$  と基数ベクトル  $B =$  ※

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (1)$$

暗号文  $C$  に対して、法  $P$ 、法  $Q$  において、それぞれ中間復号文  $M_P$ 、 $M_Q$  を式 (m)、式 (n) のようにして求めるステップと、

$$M_P \equiv w^{-1} C \pmod{P} \quad \dots (m)$$

$$M_Q \equiv w^{-1} C \pmod{Q} \quad \dots (n)$$

この中間復号文  $M_P$ 、 $M_Q$  を以下のアルゴリズムにより復号して平文ベクトル  $m = (m_0, m_1, \dots, m_{K-1})$  を求めるステップと

ステップ 0

$$M_{P0} = M_P / b_{P0}$$

$$M_{Q0} = M_Q / b_{Q0}$$

$$m_0^{(P)} \equiv M_{P0} \pmod{b_{P1}}$$

$$m_0^{(Q)} \equiv M_{Q0} \pmod{b_{Q1}}$$

中国人の剰余定理により  $m_0$  を求める。

ステップ  $i$  ( $i = 1 \sim K-2$ )

$$M_{Pi} = (M_{Pi-1} - m_{i-1}^{(P)}) / b_{Pi}$$

$$M_{Qi} = (M_{Qi-1} - m_{i-1}^{(Q)}) / b_{Qi}$$

$$m_i^{(P)} \equiv M_{Pi} \pmod{b_{Pi+1}}$$

$$m_i^{(Q)} \equiv M_{Qi} \pmod{b_{Qi+1}}$$

中国人の剰余定理により  $m_i$  を求める。

ステップ  $K-1$

$$m_{K-1} = (M_{PK-2} - m_{K-2}) / b_{PK-1}$$

または

$$* \gcd(v_i, b_{i+1}) = 1$$

$w < P$  ( $P$  : 素数) を満たす  $w$  を選択し、式 (h) により公開鍵ベクトル  $c = (c_0, c_1, \dots, c_{K-1})$  を求めるステップと、

$$c_i \equiv w B_i \pmod{P} \quad \dots (h)$$

平文ベクトル  $m$  と公開鍵ベクトル  $c$  との内積により、式 (i) に示す暗号文  $C$  を作成するステップと、

※ ( $B_0, B_1, \dots, B_{K-1}$ ) とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

素数  $P$ 、 $Q$  を設定するステップと、

基数ベクトル  $B_{Pi}$  ( $0 \leq i \leq K-1$ ) を整数  $b_{Pi}$  を用いて  $B_{Pi} = b_{P0} b_{P1} \dots b_{Pi}$  に設定するステップと、

基数ベクトル  $B_{Qi}$  ( $0 \leq i \leq K-1$ ) を整数  $b_{Qi}$  を用いて  $B_{Qi} = b_{Q0} b_{Q1} \dots b_{Qi}$  に設定するステップと、

中国人の剰余定理を用いて、 $P$ 、 $Q$  による余りがそれぞれ  $B_{Pi}$ 、 $B_{Qi}$  となるような最小の整数  $B_i$  を導くステップと、

20  $w < N$  ( $N = PQ$ ) を満たす  $w$  を選択し、式 (k) により公開鍵ベクトル  $c = (c_0, c_1, \dots, c_{K-1})$  を求めるステップと、

$$c_i \equiv w B_i \pmod{N} \quad \dots (k)$$

平文ベクトル  $m$  と公開鍵ベクトル  $c$  との内積により、式 (1) に示す暗号文  $C$  を作成するステップと、

$$m_{K-1} = (M_{QK-2} - m_{K-2}) / b_{QK-1}$$

を有することを特徴とする暗号化・復号方法。

30 【請求項 11】 前記  $N$  を法として前記暗号文  $C$  を送るようにした請求項 10 記載の暗号化・復号方法。

【請求項 12】 複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項 1、2、4、5 または 6 の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文を元の平文に復号する復号器とを備えることを特徴とする暗号通信システム。

【発明の詳細な説明】

40 【0001】

【発明の属する技術分野】 本発明は、平文を暗号文に変換するための暗号化方法、及び、暗号文を元の平文に変換するための復号方法に関し、特に、積和型暗号に関する。

【0002】

【従来の技術】 高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困

難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」、「マルチアクセス」、「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【0003】暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【0004】暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者と同じ鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【0005】これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【0006】

【発明が解決しようとする課題】公開鍵暗号系の1つである積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。

【0007】本発明は斯かる事情に鑑みてなされたものであり、多進法を用いることにより、高速な復号処理が可能である、積和型暗号における新規の暗号化方法及び復号方法を提供することを目的とする。

【0008】

【課題を解決するための手段】請求項1に係る暗号化方法は、平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と

$$C = m_0 \cdot c_0 + m_1 \cdot c_1 + \dots + m_{K-1} \cdot c_{K-1} \quad \dots (b)$$

暗号文Cに対して、中間復号文Mを式(c)のようにし

$m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて暗号文 $C = m_0 \cdot B_0 + m_1 \cdot B_1 + \dots + m_{K-1} \cdot B_{K-1}$ を得る暗号化方法において、前記 $B_i$  ( $0 \leq i \leq K-1$ )を整数 $b_i$ を用いて $B_i = b_0 \cdot b_1 \dots b_i$ に設定することを特徴とする。

【0009】請求項2に係る暗号化方法は、請求項1において、前記Kは2のべき乗数であることを特徴とする。

【0010】請求項3に係る復号方法は、請求項1によって暗号化された前記暗号文Cを復号する復号方法であって、以下のアルゴリズムにより暗号文Cから平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求めることを特徴とする。

ステップ0

$$C_0 = C / b_0$$

$$m_0 \equiv C_0 \pmod{b_1}$$

ステップi ( $i = 1 \sim K-2$ )

$$C_i = (C_{i-1} - m_{i-1}) / b_i$$

$$m_i \equiv C_i \pmod{b_{i+1}}$$

20 ステップK-1

$$m_{K-1} = (C_{K-2} - m_{K-2}) / b_{K-1}$$

【0011】請求項4に係る暗号化方法は、平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて暗号文 $C = m_0 \cdot B_0 + m_1 \cdot B_1 + \dots + m_{K-1} \cdot B_{K-1}$ を得る暗号化方法において、前記 $B_i$  ( $0 \leq i \leq K-1$ )を整数 $b_i$ 、乱数 $v_i$ を用いて $B_i = v_i \cdot b_0 \cdot b_1 \dots b_i$ に設定することを特徴とする。

【0012】請求項5に係る暗号化方法は、請求項1において、乱数ベクトル $v = (v_0, v_1, \dots, v_{K-1})$ を用いて暗号文 $C = m_0 \cdot v_0 \cdot B_0 + m_1 \cdot v_1 \cdot B_1 + \dots + m_{K-1} \cdot v_{K-1} \cdot B_{K-1}$ を得ることを特徴とする。

【0013】請求項6に係る暗号化方法は、請求項1または4において、前記K個の $b_i$ の集合を複数組準備し、それぞれの集合毎に暗号文を得るようにしたことを特徴とする。

【0014】請求項7に係る暗号化・復号方法は、平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて前記平文を暗号文に変換し、その暗号文を元の平文に変換する暗号化・復号方法において、前記 $B_i$  ( $0 \leq i \leq K-1$ )を整数 $b_i$ を用いて $B_i = b_0 \cdot b_1 \dots b_i$ に設定するステップと、 $w < P$  ( $P$ :素数)を満たす $w$ を選択し、式(a)により公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求めるステップと、 $c_i \equiv w \cdot B_i \pmod{P} \quad \dots (a)$

平文ベクトル $m$ と公開鍵ベクトル $c$ との内積により、式(b)に示す暗号文Cを作成するステップと、

50 て求めるステップと、

$$M \equiv w^{-1}C \pmod{P} \quad \dots (c)$$

この中間復号文Mを以下のアルゴリズムにより復号して  
平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求める  
ステップと

ステップ0

$$M_0 = M / b_0$$

$$m_0 \equiv M_0 \pmod{b_1}$$

ステップi (i = 1 ~ K-2)

$$M_i = (M_{i-1} - m_{i-1}) / b_i$$

$$m_i \equiv M_i \pmod{b_{i+1}}$$

ステップK-1

$$m_{K-1} = (M_{K-2} - m_{K-2}) / b_{K-1}$$

を有することを特徴とする。

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (e)$$

暗号文Cに対して、中間復号文Mを式(f)のようにし  
て求めるステップと、

$$M \equiv w^{-1}C \pmod{P} \quad \dots (f)$$

この中間復号文Mを以下のアルゴリズムにより復号して  
平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求める  
ステップと

[2分割アルゴリズム]

第1ステップ

$$ML \equiv M \pmod{B_{K/2}}$$

第2ステップ

$$MR = (M - ML) / B_{K/2}$$

[高速アルゴリズム] ML, MR に対して再び2分割アル  
ゴリズムを適用する。4分割された中間復号文のそれ  
ぞれに再び2分割アルゴリズムを適用する。このような  
ことを繰り返すを有することを特徴とする。

【0016】請求項9に係る暗号化・復号方法は、平文※30

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (i)$$

暗号文Cに対して、中間復号文Mを式(j)のようにし  
て求めるステップと、

$$M \equiv w^{-1}C \pmod{P} \quad \dots (j)$$

この中間復号文Mを以下のアルゴリズムにより復号して  
平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ を求める  
ステップと

ステップ0

$$M_0 = C / b_0$$

$$m_0 \equiv M_0 v_0^{-1} \pmod{b_1}$$

ステップi (i = 1 ~ K-2)

$$M_i = (M_{i-1} - m_{i-1} v_{i-1}) / b_i$$

$$m_i \equiv M_i v_i^{-1} \pmod{b_{i+1}}$$

ステップK-1

$$M_{K-1} = (M_{K-2} - m_{K-2} v_{K-2}) / b_{K-1}$$

$$m_{K-1} = M_{K-1} / v_{K-1}$$

を有することを特徴とする。

【0017】請求項10に係る暗号化方法・復号方法は、★

$$C = m_0 c_0 + m_1 c_1 + \dots + m_{K-1} c_{K-1} \quad \dots (l)$$

暗号文Cに対して、法P, 法Qにおいて、それぞれ中間 50 復号文 $M_P, M_Q$ を式(m), 式(n)のようにして求

\*【0015】請求項8に係る暗号化方法・復号方法は、  
平文をK (Kは2のべき乗数) 分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて前記平文を暗号文に  
変換し、前記暗号文を元の平文に変換する暗号化・復号  
方法において、前記 $B_i$  ( $0 \leq i \leq K-1$ ) を整数 $b_i$   
を用いて $B_i = b_0 b_1 \dots b_i$ に設定するステップと、  
 $w < P$  (P: 素数) を満たすwを選択し、式(d)によ  
り公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求  
めるステップと、

$$c_i \equiv w B_i \pmod{P} \quad \dots (d)$$

平文ベクトルmと公開鍵ベクトルcとの内積により、式  
(e)に示す暗号文Cを作成するステップと、

\*

※をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$   
とを用いて前記平文を暗号文に変換し、前記暗号文を元  
の平文に変換する暗号化・復号方法において、前記 $B_i$   
( $0 \leq i \leq K-1$ ) を式(g)にて設定するステップ

20 と、

$$B_i = v_i b_0 b_1 \dots b_i \quad \dots (g)$$

但し、 $v_i$ : 乱数

$b_i$ : 整数

$$\gcd(v_i, b_{i+1}) = 1$$

$w < P$  (P: 素数) を満たすwを選択し、式(h)によ  
り公開鍵ベクトル $c = (c_0, c_1, \dots, c_{K-1})$ を求  
めるステップと、

$$c_i \equiv w B_i \pmod{P} \quad \dots (h)$$

平文ベクトルmと公開鍵ベクトルcとの内積により、式  
(i)に示す暗号文Cを作成するステップと、

★平文をK分割した平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$ と基数ベクトル $B = (B_0, B_1, \dots, B_{K-1})$ とを用いて前記平文を暗号文に変換し、前記暗  
号文を元の平文に変換する暗号化・復号方法において、  
素数P, Qを設定するステップと、基数ベクトル $B_{Pi}$  ( $0 \leq i \leq K-1$ ) を整数 $b_{Pi}$ を用いて $B_{Pi} = b_{P0} b_{P1} \dots b_{Pi}$ に設定するステップと、基数ベクトル $B_{Qi}$  ( $0 \leq i \leq K-1$ ) を整数 $b_{Qi}$ を用いて $B_{Qi} = b_{Q0} b_{Q1} \dots b_{Qi}$ に設定するステップと、中国人の剰余定理を用いて、  
P, Qによる余りがそれぞれ $B_{Pi}, B_{Qi}$ となるような最  
小の整数 $B_i$ を導くステップと、 $w < N$  ( $N = PQ$ ) を  
満たすwを選択し、式(k)により公開鍵ベクトル $c =$   
 $(c_0, c_1, \dots, c_{K-1})$ を求めるステップと、

$$c_i \equiv w B_i \pmod{N} \quad \dots (k)$$

平文ベクトルmと公開鍵ベクトルcとの内積により、式  
(l)に示す暗号文Cを作成するステップと、

めるステップと、

$$M_P \equiv w^{-1}C \pmod{P} \quad \dots (m)$$

$$M_Q \equiv w^{-1}C \pmod{Q} \quad \dots (n)$$

この中間復号文 $M_P$ ,  $M_Q$ を以下のアルゴリズムにより復号して平文ベクトル $m = (m_0, m_1, \dots, m_{K-1})$

を求めるステップと

ステップ0

$$M_{P0} = M_P / b_{P0}$$

$$M_{Q0} = M_Q / b_{Q0}$$

$$m_0^{(P)} \equiv M_{P0} \pmod{b_{P1}}$$

$$m_0^{(Q)} \equiv M_{Q0} \pmod{b_{Q1}}$$

中国人の剰余定理により $m_0$ を求める。

ステップ $i$  ( $i = 1 \sim K-2$ )

$$M_{Pi} = (M_{Pi-1} - m_{i-1}) / b_{Pi}$$

$$M_{Qi} = (M_{Qi-1} - m_{i-1}) / b_{Qi}$$

$$m_i^{(P)} \equiv M_{Pi} \pmod{b_{Pi+1}}$$

$$m_i^{(Q)} \equiv M_{Qi} \pmod{b_{Qi+1}}$$

中国人の剰余定理により $m_i$ を求める。

ステップ $K-1$

$$m_{K-1} = (M_{PK-2} - m_{K-2}) / b_{PK-1}$$

または

$$M = m_0 B_0 + m_1 B_1 + \dots + m_{K-1} B_{K-1} \quad \dots (1)$$

【0022】式(1)において、 $B_i = 2^i$ である場合にはメッセージは通常の2進数で表されていることになり、 $B_i = 10^i$ である場合にはメッセージは通常の10進数で表されていることになる。

【0023】ここで、上記 $B_i$ を下記式(2)のように設定する場合を考える。

$$B_i = b_0 b_1 \dots b_i \quad \dots (2)$$

式(2)において、 $b_0 = 1$ ,  $b_i = 2$  ( $1 \leq i \leq K-1$ )と設定すると2進数の場合に一致し、 $b_0 = 1$ ,  $b_i = 10$  ( $1 \leq i \leq K-1$ )と設定すると10進数の場合に一致する。

【0024】本発明では、このような多進法を用い、つまり、式(1)及び式(2)を利用して、暗号文を作成する。

【0025】そして、基数を式(2)で与えた場合には、以下に示すアルゴリズムにより、整数 $M$ からメッセージ $m = (m_0, m_1, \dots, m_{K-1})$ を復号することができる。この復号アルゴリズムを逐次復号アルゴリズムIという。

【0026】〔逐次復号アルゴリズムI〕

ステップ0

$$M_0 = M / b_0$$

$$m_0 \equiv M_0 \pmod{b_1}$$

ステップ $i$  ( $i = 1 \sim K-2$ )

$$M_i = (M_{i-1} - m_{i-1}) / b_i$$

$$m_i \equiv M_i \pmod{b_{i+1}}$$

ステップ $K-1$

$$m_{K-1} = (M_{K-2} - m_{K-2}) / b_{K-1}$$

$$* m_{K-1} = -(M_{QK-2} - m_{K-2}) / b_{QK-1}$$

を有することを特徴とする。

【0018】請求項11に係る暗号化・復号方法は、請求項10において、前記 $N$ を法として前記暗号文 $C$ を送るようにしたことを特徴とする。

【0019】請求項12に係る暗号通信システムは、複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項1, 2, 4, 5または6の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文を元の平文に復号する復号器とを備えることを特徴とする。

【0020】本発明の暗号化方法・復号方法の概念について、以下に説明する。本発明では、多進法を用いる。

【0021】メッセージ $m = (m_0, m_1, \dots, m_{K-1})$ を基数 $B = (B_0, B_1, \dots, B_{K-1})$ を用いて、下記式(1)に示すように、整数として表記することができる。なお、ここでは、 $m_i B_i < B_{i+1}$ が成立するものとする。

\*

なお、このアルゴリズムにあつては、 $m_j < b_{j+1}$ でないと、 $m_j$ が一意に復号されない。

【0027】このような多進法による暗号化手法とそれに対する復号方法とを、本発明の特徴とする。なお、具体的な手法については後述する。

【0028】

【発明の実施の形態】以下、本発明の実施の形態について具体的に説明する。図1は、本発明による暗号化方法・復号方法をエンティティ $a$ ,  $b$ 間の情報通信に利用した状態を示す模式図である。図1の例では、一方のエンティティ $a$ が、暗号化器1にて平文 $x$ を暗号文 $C$ に暗号化し、通信路3を介してその暗号文 $C$ を他方のエンティティ $b$ へ送信し、エンティティ $b$ が、復号器2にてその暗号文 $C$ を元の平文 $x$ に復号する場合を示している。なお、復号器2には、後述する復号処理時に利用されるカウンタ2aが内蔵されている。

【0029】(第1実施の形態)秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵:  $\{b_i\}$ ,  $P$ ,  $w$

・公開鍵:  $\{c_i\}$

前記式(2)のように基数を与え、 $w < P$  ( $P$ は大きな素数)を満たす整数 $w$ をランダムに選び、式(3)を導く。

$$c_i \equiv w B_i \pmod{P} \quad \dots (3)$$

公開鍵ベクトル $c$ は、式(4)のように与えられる。

$$c = (c_0, c_1, \dots, c_{K-1}) \quad \dots (4)$$

【0030】また、 $\mu < \min(b_1, \dots, b_{K-1})$ なる $\mu$ が各エンティティに公開される。エンティティ $a$ 側

で、この公開された $\mu$ に基づいて、 $K$ 次元の $\mu$ 以下の大きさのメッセージベクトルに平文 $x$ を分割する。このようにメッセージのビット数を制限すると、 $b_0, b_1, \dots, b_{K-1}$ の大小関係は任意に設定して良い。そして、\*

$$C = m_0 \cdot c_0 + m_1 \cdot c_1 + \dots + m_{K-1} \cdot c_{K-1} \quad \dots (5)$$

【0031】なお、この暗号化は、 $K$ 重の並列処理による乗算1回、更に $\log_2 K$ 回の加算処理の所要時間で実行される。

【0032】エンティティ $b$ 側では、以下のようにして復号処理が行われる。暗号文 $C$ に対して、中間復号文 $M$ ※10

$$M = m_0 \cdot b_0 + m_1 \cdot b_0 \cdot b_1 + \dots + m_{K-1} \cdot b_0 \cdot b_1 \cdot \dots \cdot b_{K-1} \quad \dots (7)$$

【0033】図2は、復号器2で行われるこの逐次復号アルゴリズムIの処理手順を示すフローチャートである。まず、カウンタ2aをリセットして、そのカウント値 $T$ を0にする(S1)。そして、ステップ0の演算を実行して $m_0$ を求めた後(S2)、カウント値 $T$ を1にする(S3)。次に、ステップ $i$ を実行して $m_i$ を求め(S4)、カウント値 $T$ を1だけインクリメントする(S5)。カウント値 $T$ が $K-1$ に達したか否かを判断し(S6)、達していない場合には(S6:NO)、S★20

$$w b_0 \cdot b_1 \cdot \dots \cdot b_j / w b_0 \cdot b_1 \cdot \dots \cdot b_{j-1} \equiv B_j / B_{j-1} \pmod{P} \quad \dots (8)$$

$$w b_0 \cdot b_1 \cdot \dots \cdot b_{j+1} / w b_0 \cdot b_1 \cdot \dots \cdot b_j \equiv B_{j+1} / B_j \pmod{P} \quad \dots (9)$$

$$(B_j)^2 - B_{j-1} \cdot B_{j+1} = N_g \quad \dots (10)$$

一方、 $b_i$ を $p^d$ の周辺でランダムに選んだ場合、1つの $b_i$ の値を総当たり的に仮定することにより、やはり $P$ が露呈する。 $b_i$ は64ビット程度以上に選ぶ必要がある。

【0035】この第1実施の形態は、0, 1ナップザック暗号を一般化した手法として位置づけることもできる。即ち、 $m_i \in GF(2)$ とすれば、超増加数列 $\{b_0, b_0 \cdot b_1, \dots, b_0 \cdot b_1 \cdot \dots \cdot b_{K-1}\}$ による0, 1ナップザック暗号に一致する。

【0036】一般に超増加数列を用いた従来の積和型暗号方式では、基数相互間に関係がなく、平文の上位桁か☆

$$ML = m_0 \cdot B_0 + \dots + m_{K/2-1} \cdot B_{K/2-1} \quad \dots (11)$$

$$MR = (m_{K/2} \cdot B_{K/2} + \dots + m_{K-1} \cdot B_{K-1}) / B_{K/2} \quad \dots (12)$$

【0038】このような2分割アルゴリズムと、それを繰り返し適用した高速アルゴリズムとを以下に示す。

【0039】〔2分割アルゴリズム〕

第1ステップ

$$ML \equiv M \pmod{B_{K/2}}$$

第2ステップ

$$MR = (M - ML) / B_{K/2}$$

【0040】〔高速アルゴリズム〕 $ML, MR$ に対して再び2分割アルゴリズムを適用する。4分割されたメッセージのそれぞれに再び2分割アルゴリズムを適用する。このようなことを繰り返す。

【0041】このようにして、 $K$ が2のべき乗である場合には、特に高速な復号処理を実現でき、この高速アルゴリズムを適用すると、前述の逐次復号アルゴリズムと

\*そのメッセージベクトル $m$ と公開鍵ベクトル $c$ との内積を式(5)のように求めて、平文 $x$ を暗号化して暗号文 $C$ を得る。作成された暗号文 $C$ は通信路3を介してエンティティ $a$ からエンティティ $b$ へ送信される。

$$C = m_0 \cdot c_0 + m_1 \cdot c_1 + \dots + m_{K-1} \cdot c_{K-1} \quad \dots (5)$$

※を式(6)のようにして求める。

$$M \equiv w^{-1} C \pmod{P} \quad \dots (6)$$

この中間復号文 $M$ は、具体的には式(7)として与えられるので、前述の逐次復号アルゴリズムIによって復号できる。

★4, S5の処理を繰り返す。 $T=1$ から $T=K-2$ までこの処理を繰り返すことによって、 $m_1$ から $m_{K-2}$ までが求まる。カウント値 $T$ が $K-1$ に達した場合には、(S6:YES)、ステップ $K-1$ を実行して $m_{K-1}$ を求める(S7)。

【0034】ところで、この第1実施の形態において、 $b_i$ が $b_i = p^d$ というような単純な形である場合には、下記式(8)、式(9)となるので、式(10)が成立して $P$ が露呈することになる。

$$w b_0 \cdot b_1 \cdot \dots \cdot b_j / w b_0 \cdot b_1 \cdot \dots \cdot b_{j-1} \equiv B_j / B_{j-1} \pmod{P} \quad \dots (8)$$

$$w b_0 \cdot b_1 \cdot \dots \cdot b_{j+1} / w b_0 \cdot b_1 \cdot \dots \cdot b_j \equiv B_{j+1} / B_j \pmod{P} \quad \dots (9)$$

$$(B_j)^2 - B_{j-1} \cdot B_{j+1} = N_g \quad \dots (10)$$

☆ら逐次復号していく必要があり、多倍長の整数を除数とする除算が必要であった。しかしながら、この $b_i$ 進数を用いた本発明の方式では、下位桁から小さい整数を法とする剰余演算及び除算を繰り返せるので、高速に復号できることが分かる。

【0037】復号の更なる高速化を図れる復号手法について、以下に説明する。中間復号文 $M$ の前半部分を $ML$ 、中間復号文 $M$ の後半部分を $B_{K/2}$ で割ったものを $MR$ とする。これらの $ML$ 及び $MR$ は具体的には、式(11)及び式(12)で示される。なお、 $K$ は2のべき乗数とする。

$$ML = m_0 \cdot B_0 + \dots + m_{K/2-1} \cdot B_{K/2-1} \quad \dots (11)$$

$$MR = (m_{K/2} \cdot B_{K/2} + \dots + m_{K-1} \cdot B_{K-1}) / B_{K/2} \quad \dots (12)$$

比べて、 $K / \log_2 K$ 倍だけ高速に復号できる。

【0042】例えば、 $b_i$ を64ビット程度の素数とし、 $K=64$ に選んだ場合に、暗号文 $C$ の大きさは4166ビットとなるが、高速アルゴリズムによる復号時間は、 $64=2^6$ であるので、 $K=6$ の場合での逐次復号アルゴリズムによる復号時間とほぼ同程度となる。即ち、約10倍高速な復号処理を行える。なお、この場合、公開鍵サイズは1キロビット程度であってかなり大きい、1ギガビット/cm<sup>2</sup>の高密度記録が可能となるような状況を考えると、この公開鍵サイズは実用上問題ないと言える。

【0043】(第2実施の形態)第1実施の形態に乱数を付加した第2実施の形態について説明する。第1実施の形態では、 $\{B_i\}$ が超増加数列になる。よって、超増加数列に対する攻撃法として有名なLLL (Lenatra-

Lenatra-Lovasz) 法による攻撃を、第1実施の形態は受け易いという可能性がある。そこで、第2実施の形態では、基数に乱数を付加する、つまり、第1実施の形態での基数ベクトルに乱数を掛け合わせたものを基数ベクトルとして使用することによって、安全性を強化する。

【0044】秘密鍵と公開鍵とを以下のように準備する。

- ・秘密鍵:  $\{b_i\}$ ,  $\{v_i\}$ ,  $P$ ,  $w$
- ・公開鍵:  $\{c_i\}$

基数  $B_i$  を式 (13) のように与える。

$$B_i = v_i \cdot b_0 \cdot b_1 \cdots b_i \quad \cdots (13)$$

ここで、式 (13) で示される各  $B_i$  がほぼ同じ大きさになるように  $v_i$  を設定する。よって、 $\{B_i\}$  は超増加数列ではなくLLL法の攻撃を受けにくい。但し、 $g \cdot c \cdot d(v_i, b_{i+1}) = 1$  を満たすものとする。

$$M = m_0 \cdot v_0 \cdot b_0 + m_1 \cdot v_1 \cdot b_0 \cdot b_1 + \cdots + m_{K-1} \cdot v_{K-1} \cdot b_0 \cdot b_1 \cdots b_{K-1} \quad \cdots (17)$$

【0048】[逐次復号アルゴリズムII]

ステップ0

$$M_0 = M / b_0$$

$$m_0 \equiv M_0 \cdot v_0^{-1} \pmod{b_1}$$

ステップi ( $i = 1 \sim K-2$ )

$$M_i = (M_{i-1} - m_{i-1} \cdot v_{i-1}) / b_i$$

$$m_i \equiv M_i \cdot v_i^{-1} \pmod{b_{i+1}}$$

ステップK-1

$$M_{K-1} = (M_{K-2} - m_{K-2} \cdot v_{K-2}) / b_{K-1}$$

$$m_{K-1} = M_{K-1} / v_{K-1}$$

【0049】なお、この逐次復号アルゴリズムIIを復号器2で実行するフローチャートは、逐次復号アルゴリズムIのフローチャート(第2図)と同様である。

【0050】ここで、第2実施の形態における具体例を示す。

・秘密鍵

$$b = (1, 11, 13)$$

$$v = (1009, 131, 7)$$

$$B = (1009, 1441, 1001)$$

$$P = 27481$$

$$w = 739$$

$$w^{-1} \equiv 702 \pmod{P}$$

( $b_1 < b_2 < b_3$  であるので、 $v_1 > v_2 > v_3$  と設定することにより、 $B_1, B_2, B_3$  が超増加数列にならないようにしている)

・公開鍵

$$c \equiv w \cdot B$$

$$\equiv (3664, 20621, 25233) \pmod{P}$$

・暗号化

メッセージを  $m = (6, 7, 8)$  とする。

$$C = c \cdot m$$

$$= 6 \times 3664 + 7 \times 20621 + 8 \times 25233$$

$$= 368195$$

\*【0045】整数  $w$  を用いて、第1実施の形態と同様に、公開鍵ベクトル  $c$  を以下の式 (14)、式 (15) のように求める。

$$c_i \equiv w \cdot B_i \pmod{P} \quad \cdots (14)$$

$$c = (c_0, c_1, \dots, c_{K-1}) \quad \cdots (15)$$

【0046】メッセージベクトル  $m$  と公開鍵ベクトル  $c$  との内積により、第1実施の形態と同様に(前記式(5))、暗号文  $C$  を得る。

【0047】復号処理は、以下のようにして行われる。

10 暗号文  $C$  に対して、中間復号文  $M$  を式 (16) のようにして求める。

$$M \equiv w^{-1} \cdot C \pmod{P} \quad \cdots (16)$$

この中間復号文  $M$  は、具体的には式 (17) として与えられるので、以下に示す逐次復号アルゴリズムIIによって復号できる。

・復号

中間復号文  $M$  を求め、逐次復号アルゴリズムIIを用いて

20 復号する。  $M \equiv w^{-1} \cdot C$

$$\equiv 702 \times 368195$$

$$\equiv 24149 \pmod{27481}$$

ステップ0

$$M_0 = 24149 / 1 = 24149$$

$$m_0 \equiv 24149 \times 1009^{-1} \equiv 6 \pmod{11}$$

ステップ1

$$M_1 = (24149 - 6 \times 1009) / 11 = 1645$$

$$m_1 \equiv 1645 \times 131^{-1} \equiv 7 \pmod{13}$$

ステップ2

30  $M_2 = (1645 - 7 \times 131) / 13 = 56$

$$m_2 = 56 / 7 = 8$$

以上のようにして、メッセージ  $m = (6, 7, 8)$  を得る。

【0051】(第3実施の形態) 第2実施の形態では、基数ベクトル自体に乱数を組み込むようにしたが、第1実施の形態と同じ基数ベクトルを使用し、暗号文  $C$  を作成する段階で乱数  $v_0, v_1, \dots, v_{K-1}$  を付加するようにすることもできる。この場合の暗号文  $C$  は、第2実施の形態と同じ形となる。

40 【0052】(第4実施の形態) 第1実施の形態で基数ベクトルを多重化した第4実施の形態について説明する。第4実施の形態は、第1実施の形態による基数ベクトル  $\{B_i\}$  を2つの法それぞれにおいて設定し、中国人の剰余定理を利用した暗号化・復号方法である。この第4実施の形態でも、基数ベクトル  $\{B_i\}$  が超増加数列とはならず、LLL法の攻撃に強い。また、平文の桁数を大きくできる。

【0053】秘密鍵と公開鍵とを以下のように準備する。

50 ・秘密鍵:  $\{b_{Pi}\}^{-1}, \{b_{Qi}\}, P, Q, N, w$



・公開鍵:  $\{c_i\}$

2つの大きな素数P, Qを選択し、それらの積をNとする。第1実施の形態におけるK個の $b_i$ の集合を2通り準備し、 $\{b_{Pi}\}$ ,  $\{b_{Qi}\}$ とする。また、それらより生成した基数を $\{B_{Pi}\}$ ,  $\{B_{Qi}\}$ とする。中国人の剰余定理を用いて、P, Qによる余りがそれぞれ $B_{Pi}$ ,  $B_{Qi}$ となるような最小の整数 $B_i$ を導く。

【0054】Nを法として、秘密の整数wを用いて、第1実施の形態と同様に、公開鍵ベクトルcを以下の式(18), 式(19)のように求める。

$$c_i \equiv w B_i \pmod{N} \quad \dots (18)$$

$$c = (c_0, c_1, \dots, c_{K-1}) \quad \dots (19) \quad *$$

$$M_P = m_0 B_{P0} + m_1 B_{P1} + \dots + m_{K-1} B_{PK-1} \quad \dots (22)$$

$$M_Q = m_0 B_{Q0} + m_1 B_{Q1} + \dots + m_{K-1} B_{QK-1} \quad \dots (23)$$

【0058】 $M_P$ ,  $M_Q$ に対して、以下に示す逐次復号アルゴリズムIIIを適用することによって、余りのペア $(m_i^{(P)}, m_i^{(Q)})$ を導くことができる。但し、 $m_i$ は、式(24), 式(25)の何れかであるとする。

$$m_i \equiv m_i^{(P)} \pmod{b_{Pi+1}} \quad \dots (24)$$

$$m_i \equiv m_i^{(Q)} \pmod{b_{Qi+1}} \quad \dots (25)$$

これらに対して中国人の剰余定理を適用すると、メッセージ $m_i < \text{lcm}(b_{Pi+1}, b_{Qi+1})$ を復号することができる。

【0059】〔逐次復号アルゴリズムIII〕

ステップ0

$$M_{P0} = M_P / b_{P0}$$

$$M_{Q0} = M_Q / b_{Q0}$$

$$m_0^{(P)} \equiv M_{P0} \pmod{b_{P1}}$$

$$m_0^{(Q)} \equiv M_{Q0} \pmod{b_{Q1}}$$

中国人の剰余定理により $m_0$ を求める。

ステップi ( $i = 1 \sim K-2$ )

$$M_{Pi} = (M_{Pi-1} - m_{i-1}) / b_{Pi}$$

$$M_{Qi} = (M_{Qi-1} - m_{i-1}) / b_{Qi}$$

$$m_i^{(P)} \equiv M_{Pi} \pmod{b_{Pi+1}}$$

$$m_i^{(Q)} \equiv M_{Qi} \pmod{b_{Qi+1}}$$

中国人の剰余定理により $m_i$ を求める。

ステップK-1

$$m_{K-1} = (M_{PK-2} - m_{K-2}) / b_{PK-1}$$

または

$$m_{K-1} = (M_{QK-2} - m_{K-2}) / b_{QK-1}$$

【0060】ここで、第4実施の形態における具体例を示す。

・秘密鍵

$$b_P = (1, 11, 19)$$

$$b_Q = (1, 13, 17)$$

$$B_P = (1, 11, 209)$$

$$B_Q = (1, 13, 221)$$

$$B = (1, 326859526, 1961157299)$$

$$P = 45053$$

$$Q = 54833$$

\* 【0055】メッセージベクトルmと公開鍵ベクトルcとの内積により、第1実施の形態と同様に(前記式(5))、暗号文Cを得る。

【0056】復号処理は、以下のようにして行われる。

暗号文Cに対して、法P, 法Qにおいて、それぞれ中間復号文 $M_P$ ,  $M_Q$ を式(20), 式(21)のようにして求める。

$$M_P \equiv w^{-1} C \pmod{P} \quad \dots (20)$$

$$M_Q \equiv w^{-1} C \pmod{Q} \quad \dots (21)$$

10 【0057】各中間復号文 $M_P$ ,  $M_Q$ に関して、式(22), 式(23)が成立する。

$$N = 2470391149$$

$$w = 320718294$$

$$w^{-1} \equiv 1798315174 \pmod{N}$$

( $B_P$ ,  $B_Q$ では超増加性が見られるが、Bは超増加数列ではない)

20 ・公開鍵

$$c \equiv w B$$

$$\equiv (320718294, 1521781250, 644798264) \pmod{N}$$

・暗号化

メッセージを $m = (45, 67, 89)$ とする。

$$C = c \cdot m$$

$$= 173778712476$$

(メッセージの分割ビット数を11×13以下まで向上できる)

・復号

30 中間復号文 $M_P$ ,  $M_Q$ を求め、逐次復号アルゴリズムIIIを用いて復号する。

$$M_P \equiv w^{-1} C \equiv 19383 \pmod{45053}$$

$$M_Q \equiv w^{-1} C \equiv 20585 \pmod{54833}$$

ステップ0

$$M_{P0} = 19383 / 1 = 19383$$

$$M_{Q0} = 20585 / 1 = 20585$$

$$m_{P0} \equiv 19383 \equiv 1 \pmod{11}$$

$$m_{Q0} \equiv 20585 \equiv 6 \pmod{13}$$

$$m_0 \equiv 45 \pmod{143}$$

40 ステップ1

$$M_{P1} = (19383 - 45) / 11 = 1758$$

$$M_{Q1} = (20585 - 45) / 13 = 1580$$

$$m_{P1} \equiv 1758 \equiv 10 \pmod{19}$$

$$m_{Q1} \equiv 1580 \equiv 16 \pmod{17}$$

$$m_1 \equiv 67 \pmod{323}$$

ステップ2

$$m_{P2} = (1758 - 67) / 19 = 89$$

$$m_{Q2} = (1580 - 67) / 17 = 89$$

$$m_2 = 89$$

50 以上のようにして、メッセージ $m = (45, 67, 89)$ を得

る。

【0061】なお、合成数 $N$ を法とする第4実施の形態のような多重化方式では、 $N$ の素因数分解が困難である場合、 $N$ を公開しても安全と考えられる。よって、そのような場合には、 $N$ を法として求めた暗号文 $C$ を送付することにより、暗号化効率が向上する。

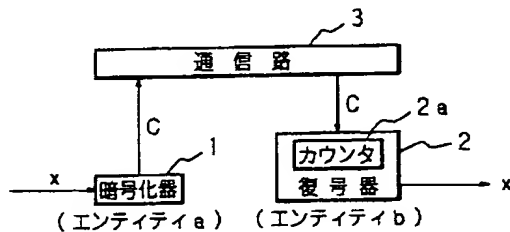
【0062】（第5実施の形態）第5実施の形態は、第4実施の形態に乱数を付加した暗号方式、言い換えると、第2実施の形態で基数ベクトルを多重化した暗号方式である。なお、この第5実施の形態については、前述

の第1～第4実施の形態を参照すれば容易にその内容が理解されるので、詳細な説明は省略する。

【0063】

【発明の効果】以上のように、本発明では、基数 $B_i$ を

【図1】



$B_i = b_0, b_1, \dots, b_i$  に設定するようにして、メッセージを多進法を用いて表現するようにしたので、高速な復号を行うことができる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図1】2人のエンティティ間における情報の通信状態を示す模式図である。

【図2】本発明における復号の処理手順を示すフローチャートである。

【符号の説明】

- 1 暗号化器
- 2 復号器
- 3 通信路
- a, b エンティティ

【図2】

